1. Let $m, k \in \mathbb{N}$, $m > 1$ and let $i + 1$ be the number of binary digits of $k$. Let $x_0 = 2^{1+\lfloor i/m \rfloor}$. Prove

$$k^{1/m} < x_0 < 2k^{1/m}.$$ 

2. Evaluate the Legendre symbols $(\frac{2}{137})$, $(\frac{3}{137})$, $(\frac{53}{137})$, $(\frac{111}{1151})$.

3. (i) Prove that $(\frac{-2}{p}) = 1 \iff p \equiv 1 \text{ or } 3 \pmod{8}$;
(ii) Prove that $(\frac{2}{p}) = 1 \iff p \equiv 1 \text{ or } 4 \pmod{5}$.

4. Apply Serret’s algorithm to express primes 137 and $10^{50} + 577$ as sums of two squares.

5. If $p$ is a prime and $p = x^2 + ny^2$, where $x, y, n \in \mathbb{Z}$, prove that $\gcd(x, y) = 1$ and $(\frac{-n}{p}) = 1$.

6. (Wilson’s theorem) Let $p$ be a prime. By grouping integers $x, y$ in the range $1 \leq x < y \leq p - 1$ as products $xy$, where $xy \equiv 1 \pmod{p}$, prove that $(p - 1)! \equiv -1 \pmod{p}$.

7. Let $p$ be an odd prime not dividing $b$. Define a 1–1 mapping $y = f(x)$ of $\{x \in \mathbb{N} \mid 1 \leq x \leq p - 1\}$ onto itself, by $xy \equiv b \pmod{p}$.

(i) If $(\frac{b}{p}) = -1$, show that the mapping has no fixed points and deduce that $(p - 1)! \equiv b^{\frac{p-1}{2}} \pmod{p}$.
(ii) If $(\frac{b}{p}) = 1$, show that the mapping has two fixed points and deduce that $(p - 1)! \equiv -b^{\frac{p-1}{2}} \pmod{p}$.

(In view of Wilson’s theorem, this gives another proof of Euler’s criterion.)
8. If $p$ is an odd prime, not dividing $k$, show that
\[
\sum_{x=1}^{p-1} \left( \frac{x(x + k)}{p} \right) = -1.
\]
(Hint: Define $y$ by $xy \equiv 1 \pmod{p}$, $1 \leq y \leq p - 1$ and write the sum as
\[
\sum_{x=1}^{p-1} \left( \frac{xy(xy + ky)}{p} \right).
\]

9. Show that 65 is a strong pseudoprime to the base 8 but not to the base 14.

10. Let $N_p$ be the number of $(x, y), 1 \leq x, y \leq p - 1$, satisfying $x^2 + y^2 \equiv 4 \pmod{p}$.
   (i) Prove that $N_p \equiv 2 + 2 \left( \frac{2}{p} \right) \pmod{8}$.
   (ii) By writing $x \equiv (2 - y)t \pmod{p}$, obtain the parametrisation
   \[
   (x, y) \equiv \left( \frac{4t}{t^2 + 1}, \frac{2(t^2 - 1)}{t^2 + 1} \right) \pmod{p},
   \]
   \[2 \leq t \leq p - 2, \quad t^2 \not\equiv -1 \pmod{p}.
   \]
   (iii) Deduce that $N_p = p - 3 - \{1 + \left( \frac{-1}{p} \right)\}$ and hence prove that
   \[
   \left( \frac{2}{p} \right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8} \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}
   \]